

# **EXHIBIT 126**

**3/12/19**  
**CHROME**  
**PRIVACY**  
**NOTICE**



This is an archived version of the Chrome privacy notice. View the current privacy notice.

# Google Chrome Privacy Notice

Archive date: March 12, 2019

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.



# Go Chrome

## Table of contents:

- Browser modes
- Managing users in Chrome
- Safe Browsing practices
- Privacy practices of using apps, extensions, themes, services, and other add-ons
- More information

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the network actions prediction feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.

## Google Chrome

- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can delete your browsing history information.
- You can manage or delete stored browsing data from the Cookies and Site Data dialog.
- You can stop Chrome from accepting cookies. Learn more.
- You can review stored passwords in Chrome settings. Learn more.
- You can view and manage your stored Autofill information. Learn more.

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync, or, in the case of payment cards and billing information, choosing specific payment card and billing information to store in your Google Payments account. Learn More.

How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive standard log information, including your system's IP address and data from cookies. In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that

## Go g e Chrome

with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more.](#)

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active

## Go g e Chrome

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the address bar in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the address bar in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill and password management.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

**Payments.** When you are signed into Chrome with your Google account, Chrome may offer to save payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you have cards saved locally in Chrome, Chrome may prompt you to save them to your Google Payments account. If you use a payment card from your Google Payments account or choose to save



## Go e Chrome

from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or

## Go e Chrome

Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more.](#)

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

### Identifiers in Chrome

Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed.

## Google Chrome

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

## Sign-in and Sync Chrome modes

You also have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.

## Go Chrome

this off in settings. [Learn more](#). If you are signed in to your Google Account on desktop, Chrome may offer to save your payment cards and related billing information to your Google Payments account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Data from Chrome sync Dashboard](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

How Chrome handles your synced information



## Go ge Chrome

your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more.](#)

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more.](#)

### Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- [Basic browsing history information](#) like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

## Go e Chrome

information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more](#).

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also

Go g e Chrome

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive standard log information, including an IP address and cookies.

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. Learn more.

The following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

## Google Chrome

settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.

- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, Chrome will also flag your Google Account as likely phished.
- You can always choose to [disable the Safe Browsing feature within Chrome](#).

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

## Managing add-ons

## Go ge Chrome

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

## Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:



## Go g e Chrome

NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. D; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time theys/he visits Google from that particular computer).

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google adheres to several self regulatory frameworks, including the EU-US Privacy Shield Framework. [Learn more](#). The Google affiliate listed as provider of the Chrome service in the [Google Chrome Terms of Service](#) shall be the data controller responsible for your information and responsible for processing your information and complying with applicable privacy laws.

# Google Chrome

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

# **EXHIBIT 127**

**10/31/19  
CHROME  
PRIVACY  
NOTICE**





This is an archived version of the Chrome privacy notice. View the current privacy notice.

# Google Chrome Privacy Notice

Archive date: October 31, 2019

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

# Go Chrome

## Table of contents:

- Browser modes
- Managing users in Chrome
- Safe Browsing practices
- Privacy practices of using apps, extensions, themes, services, and other add-ons
- More information

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the network actions prediction feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.

## Google Chrome

- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can delete your browsing history information.
- You can manage or delete stored browsing data from the Cookies and Site Data dialog.
- You can stop Chrome from accepting cookies. Learn more.
- You can review stored passwords in Chrome settings. Learn more.
- You can view and manage your stored Autofill information. Learn more.

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync, or, in the case of payment cards and billing information, choosing specific payment card and billing information to store in your Google Payments account. Learn More.

How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive standard log information, including your system's IP address and data from cookies. In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that

## Go Chrome

with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more.](#)

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active

## Go g e Chrome

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the address bar in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the address bar in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill and password management.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

**Payments.** When you are signed into Chrome with your Google account, Chrome may offer to save payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you have cards saved locally in Chrome, Chrome may prompt you to save them to your Google Payments account. If you use a payment card from your Google Payments account or choose to save



## Go Chrome

from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web

## Go ge Chrome

identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

### Identifiers in Chrome

Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. For example, if you use push messaging, an

## Google Chrome

Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

## Sign-in and Sync Chrome modes



## Go e Chrome

**Sign in on Desktop.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). If you are signed in to your Google Account on desktop, Chrome may offer to save your payment cards and related billing information to your Google Payments account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Data from Chrome sync Dashboard](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

## Go Chrome

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more.](#)

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more.](#)

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- [Basic browsing history information](#) like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

## Go Chrome

information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more](#).

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also

Go g e Chrome

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive standard log information, including an IP address and cookies.

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. Learn more.

The following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.



## Google Chrome

settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.

- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, Chrome will also flag your Google Account as likely phished.
- You can always choose to [disable the Safe Browsing feature within Chrome](#).

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

## Managing add-ons

## Go Chrome

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

## Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

## Google Chrome

NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. D; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time theys/he visits Google from that particular computer).

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google complies with certain [legal frameworks](#) relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Framework. [Learn more](#). The Google affiliate listed as provider of the Chrome service in the [Google Chrome Terms of Service](#) shall be the data controller responsible for your information and responsible for processing your information and complying with applicable privacy laws.

# Google Chrome

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.



# **EXHIBIT 128**

**12/10/19  
CHROME  
PRIVACY  
NOTICE**



This is an archived version of the Chrome privacy notice. View the current privacy notice.

# Google Chrome Privacy Notice

Archive date: December 10, 2019

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

# Go g e Chrome

## Table of contents:

- Browser modes
- Managing users in Chrome
- Safe Browsing practices
- Privacy practices of using apps, extensions, themes, services, and other add-ons
- More information

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the network actions prediction feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.

## Google Chrome

- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can delete your browsing history information.
- You can manage or delete stored browsing data from the Cookies and Site Data dialog.
- You can stop Chrome from accepting cookies. Learn more.
- You can review stored passwords in Chrome settings. Learn more.
- You can view and manage your stored Autofill information. Learn more.

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync, or, in the case of payment cards and billing information, choosing specific payment card and billing information to store in your Google Payments account. Learn More.

How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive standard log information, including your system's IP address and data from cookies. In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that

## Go g e Chrome

with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more.](#)

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active



## Go g e Chrome

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill and password management.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

**Payments.** When you are signed into Chrome with your Google account, Chrome may offer to save payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you have cards saved locally in Chrome, Chrome may prompt you to save them to your Google Payments account.

## Go g e Chrome

collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash

## Go Chrome

the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

Identifiers in Chrome



## Go g e Chrome

identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed.

Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

## Sign-in and Sync Chrome modes

## Go e Chrome

**Sign in on Desktop.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). If you are signed in to your Google Account on desktop, Chrome may offer to save your payment cards and related billing information to your Google Payments account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Data from Chrome sync Dashboard](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.



## Go Chrome

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more.](#)

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more.](#)

### Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- [Basic browsing history information](#) like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

## Go e Chrome

information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also

Go  ge Chrome

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive standard log information, including an IP address and cookies.

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. Learn more.

The following Safe Browsing features are specific to Chrome:

- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. This feature is disabled in incognito and guest modes.

## Go ge Chrome

known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).



## Go ge Chrome

Apple controls the Safe Browsing technology used by your device and may send data to Safe Browsing providers other than Google.

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

## Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.



## Go g e Chrome

agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

### Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
https://www.google.com/search?q=cars - Firefox 1.0.7; Windows
NT 5.1 - 740674ce2123e969
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID

Go g e Chrome

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google complies with certain [legal frameworks](#) relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Framework. [Learn more](#). The Google affiliate listed as provider of the Chrome service in the [Google Chrome Terms of Service](#) shall be the data controller responsible for your information and responsible for processing your information and complying with applicable privacy laws.

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. [Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.](#)

### Google Account

## Go ge Chrome

and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

# **EXHIBIT 129**

**3/17/20  
CHROME  
PRIVACY  
NOTICE**



This is an archived version of the Chrome privacy notice. View the current privacy notice.

# Google Chrome Privacy Notice

Archive date: March 17, 2020

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.



# Go Chrome

## Table of contents:

- Browser modes
- Managing users in Chrome
- Safe Browsing practices
- Privacy practices of using apps, extensions, themes, services, and other add-ons
- More information

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the network actions prediction feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.

## Google Chrome

- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can delete your browsing history information.
- You can manage or delete stored browsing data from the Cookies and Site Data dialog.
- You can stop Chrome from accepting cookies. Learn more.
- You can review stored passwords in Chrome settings. Learn more.
- You can view and manage your stored Autofill information. Learn more.

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync, or, in the case of payment cards and billing information, choosing specific payment card and billing information to store in your Google Payments account. Learn More.

How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive standard log information, including your system's IP address and data from cookies. In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that

## Go Chrome

with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more.](#)

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active

## Go g e Chrome

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill and password management.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

**Payments.** When you are signed into Chrome with your Google account, Chrome may offer to save payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you have cards saved locally in Chrome, Chrome may prompt you to save them to your Google Payments account.



## Go g e Chrome

collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash



## Go g e Chrome

the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

Identifiers in Chrome

## Go g e Chrome

identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed.

Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

## Sign-in and Sync Chrome modes

## Go e Chrome

**Sign in on Desktop.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). If you are signed in to your Google Account on desktop, Chrome may offer to save your payment cards and related billing information to your Google Payments account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Data from Chrome sync Dashboard](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

## Go ge Chrome

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more.](#)

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more.](#)

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- [Basic browsing history information](#) like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.



## Go e Chrome

information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more](#).

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also



Go g e Chrome

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive standard log information, including an IP address and cookies.

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. Learn more.

The following Safe Browsing features are specific to Chrome:

- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. This feature is disabled in incognito and guest modes.

## Go ge Chrome

known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).

## Go ge Chrome

Apple controls the Safe Browsing technology used by your device and may send data to Safe Browsing providers other than Google.

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

## Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

## Go Chrome

agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

### Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -  
https://www.google.com/search?q=cars - Firefox 1.0.7; Windows  
NT 5.1 - 740674ce2123e969
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID



Go  Chrome

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google complies with certain [legal frameworks](#) relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Framework. [Learn more](#).

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and [how Google uses data, including cookies, when you use our partners' sites or apps](#).

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by



Go  Chrome

# **EXHIBIT 130**

**5/20/20  
CHROME  
PRIVACY  
NOTICE**



# Google Chrome Privacy Notice

Last modified: May 20, 2020

View archived versions:  ▼

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.



## Table of contents:

- Browser modes
- Managing users in Chrome
- Safe Browsing practices
- Privacy practices of using apps, extensions, themes, services, and other add-ons
- More information

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the network actions prediction feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.

## ≡ Go g e Chrome

- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can delete your browsing history information.
- You can manage or delete stored browsing data from the Cookies and Site Data dialog.
- You can stop Chrome from accepting cookies. Learn more.
- You can review stored passwords in Chrome settings. Learn more.
- You can view and manage your stored Autofill information. Learn more.

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync, or, in the case of payment cards and billing information, choosing specific payment card and billing information to store in your Google Payments account. Learn More.

How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive standard log information, including your system's IP address and data from cookies. In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that





with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more.](#)

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active



**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill and password management.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

**Payments.** When you are signed into Chrome with your Google account, Chrome may offer to save payment cards and related billing information to your Google Payments account. Chrome may also offer you the option of filling payment cards from your Google Payments account into web forms. If you have cards saved locally in Chrome, Chrome may prompt you to save them to your Google Payments account.

## ≡ Go g e Chrome

collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash



## ≡ Go g e Chrome

the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

Identifiers in Chrome

## ≡ Go g e Chrome

identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed.

Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

Sign-in and Sync Chrome modes





**Sign in on Desktop.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). If you are signed in to your Google Account on desktop, Chrome may offer to save your payment cards and related billing information to your Google Payments account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Data from Chrome sync Dashboard](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

## ≡ Go g e Chrome

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more.](#)

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more.](#)

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- [Basic browsing history information](#) like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.



information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also



## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive standard log information, including an IP address and cookies.

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. Learn more.

The following Safe Browsing features are specific to Chrome:

- If you have turned on Safe Browsing's Enhanced Protection mode, Chrome provides additional protections, and sends Google additional data, as described in Chrome settings. Learn more. Some of these protections may also be available as standalone features, subject to separate controls, where Standard Protection is enabled.



## ≡ Go **g**e Chrome

Google the full URL of each site you visit to determine whether that site is safe. If you also sync your browsing history without a sync passphrase, these URLs will be temporarily associated with your Google account to provide more personalized protection. This feature is disabled in incognito and guest modes.

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.
- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data



## ≡ Go ge Chrome

and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).

- On desktop and Android versions of Chrome, you can always choose to disable the Safe Browsing feature within Chrome settings. On iOS versions of Chrome, Apple controls the Safe Browsing technology used by your device and may send data to Safe Browsing providers other than Google.

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

### Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

## ≡ Go g e Chrome

- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

## Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
https://www.google.com/search?q=cars - Firefox 1.0.7; Windows
NT 5.1 - 740674ce2123e969
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;

## ≡ Go g e Chrome

- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time theys/he visits Google from that particular computer).

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google complies with certain [legal frameworks](#) relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Framework. [Learn more](#).

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not



## Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

Follow us



Chrome Family



Enterprise



Education



Dev and Partners



Stay Connected



≡ Go ge Chrome



[Privacy and Terms](#)

[About Google](#)

[Google Products](#)



[Help](#)

[English - United States](#)



# **EXHIBIT 131**

**1/15/21  
CHROME  
PRIVACY  
NOTICE**

This is an archived version of the Chrome privacy notice. [View the current privacy notice.](#)

# Google Chrome Privacy Notice

Archive date: January 15, 2021

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, ChromeOS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

- [Managing users in Chrome](#)
- [Safe Browsing practices](#)
- [Privacy practices of using apps, extensions, themes, services, and other add-ons](#)
- [More information](#)

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.
- [Cookies](#) or data from websites that you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

- You can [delete your browsing history information](#).
- You can manage or delete stored browsing data from the [Cookies and Site Data dialog](#).
- You can stop Chrome from [accepting cookies](#). [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by turning on sync, or, in the case of passwords, payment cards, and billing information, choosing specific credentials or payment card and billing information to store in your Google Account. [Learn More](#).

## How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, Chrome automatically shares your location with your default search engine if the Chrome app has permission to access your location and you haven't blocked geolocation for the associated web site. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).



Chrome sends Google the URL of the page you're trying to reach.

**Autofill, password management, and payments.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more.](#)

When you are signed into Chrome with your Google Account, Chrome may offer to save passwords, payment methods and related information to your Google Account. Chrome may also offer you the option of filling passwords and payment methods from your Google Account into web forms. If you have passwords or payment methods saved locally in Chrome, Chrome may prompt you to save them to your Google Account. If you use a payment method from your Google Account or choose to save your payment method in your Google Account for future use, Chrome will collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls.](#)

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more.](#)

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as

"Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on ChromeOS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You

## Identifiers in Chrome

Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. ChromeOS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

with or without sync enabled.

**Sign in.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). On Chrome on Android, when you sign into any Google web service, Chrome may offer to sign you in with the Google Accounts that are already signed in on the device. You can turn this off in settings. [Learn more](#). If you are signed in to Chrome with your Google Account, Chrome may offer to save your passwords, payment methods and related information to your Google Account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it at [Chrome data from your account](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The

## How Chrome handles your synced information

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more.](#)

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more.](#)

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- [Basic browsing history information](#) like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

## How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.



are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

---

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system.

[Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for ChromeOS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more](#).

The following Safe Browsing features are specific to Chrome:

- If you have turned on Safe Browsing's Enhanced Protection mode, Chrome provides additional protections, and sends Google additional data, as described in Chrome settings. [Learn more](#). Some of these protections may also be available as standalone features, subject to separate controls, where Standard Protection is enabled.
- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. If you also sync your browsing history without a sync passphrase, these URLs will be temporarily associated with your Google account to provide more personalized protection. This feature is disabled in incognito and guest modes.

URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).
- On desktop and Android versions of Chrome, you can always choose to [disable the Safe Browsing feature within Chrome settings](#). On iOS versions of Chrome, Apple controls

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

### Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

## Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

123.45.67.89 - 25/Mar/2003 10:15:32 - https://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time they/s/he visits Google from that particular computer).

---

## More information





including [cookies](#), is subject to the privacy policies of those websites.

Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in the [Google Privacy Policy](#). We also comply with certain legal frameworks relating to the transfer of data, including the European frameworks described on our [Data Transfer Frameworks page](#). [Learn more](#).

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

## Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

# **EXHIBIT 132**

**9/23/21  
CHROME  
PRIVACY  
NOTICE**

This is an archived version of the Chrome privacy notice. [View the current privacy notice.](#)

# Google Chrome Privacy Notice

Archive date: September 23, 2021

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, ChromeOS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

- [Managing users in Chrome](#)
- [Safe Browsing practices](#)
- [Privacy practices of using apps, extensions, themes, services, and other add-ons](#)
- [More information](#)

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.
- [Cookies](#) or data from websites that you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

- You can [delete your browsing history information](#).
- You can manage or delete stored browsing data from the [Cookies and Site Data dialog](#).
- You can stop Chrome from [accepting cookies](#). [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by turning on sync, or, in the case of passwords, payment cards, and billing information, choosing specific credentials or payment card and billing information to store in your Google Account. [Learn More](#).

## How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site



**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more.](#)

When you are signed into Chrome with your Google Account, Chrome may offer to save passwords, payment methods and related information to your Google Account. Chrome may also offer you the option of filling passwords and payment methods from your Google Account into web forms. If you have passwords or payment methods saved locally in Chrome, Chrome may prompt you to save them to your Google Account. If you use a payment method from your Google Account or choose to save your payment method in your Google Account for future use, Chrome will collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls.](#)

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more.](#)

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If

demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on ChromeOS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

## Identifiers in Chrome

to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. ChromeOS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

## Sign-in and Sync Chrome modes

You also have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.

Chrome on Android and iOS, when you sign into any Google web service, Chrome may offer to sign you in with the Google Accounts that are already signed in on the device. You can turn this off in settings. [Learn more](#). If you are signed in to Chrome with your Google Account, Chrome may offer to save your passwords, payment methods and related information to your Google Account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it at [Chrome data from your account](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required and sync cannot be disabled because it provides parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

## How Chrome handles your synced information



Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more](#).

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more](#).

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- **Basic browsing history information** like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

## How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

**Browser configuration changes.** When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

---

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system.

[Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for ChromeOS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

---

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about

## How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more](#).

The following Safe Browsing features are specific to Chrome:

- If you have turned on Safe Browsing's Enhanced Protection mode, Chrome provides additional protections, and sends Google additional data, as described in Chrome settings. [Learn more](#). Some of these protections may also be available as standalone features, subject to separate controls, where Standard Protection is enabled.
- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. If you also sync your browsing history without a sync passphrase, these URLs will be temporarily associated with your Google account to provide more personalized protection. This feature is disabled in incognito and guest modes.
- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.

- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).
- On desktop and Android versions of Chrome, you can always choose to [disable the Safe Browsing feature within Chrome settings](#). On iOS versions of Chrome, Apple controls the Safe Browsing technology used by your device and may send data to Safe Browsing providers other than Google.

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

### Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.



sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

123.45.67.89 - 25/Mar/2003 10:15:32 - https://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time they/he visits Google from that particular computer).

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.



the [Google Privacy Policy](#). We also comply with certain legal frameworks relating to the transfer of data, including the European frameworks described on our [Data Transfer Frameworks page](#). [Learn more](#).

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

## Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

# **EXHIBIT 133**

**6/23/22**

## **CHROME PRIVACY NOTICE**

This is an archived version of the Chrome privacy notice. [View the current privacy notice.](#)

# Google Chrome Privacy Notice

Archive date: June 23, 2022

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, ChromeOS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

- [Managing users in Chrome](#)
- [Safe Browsing practices](#)
- [Privacy practices of using apps, extensions, themes, services, and other add-ons](#)
- [More information](#)

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.
- [Cookies](#) or data from websites that you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.



- You can [delete your browsing history information](#).
- You can manage or delete stored browsing data from the [Cookies and Site Data dialog](#).
- You can stop Chrome from [accepting cookies](#). [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by turning on sync, or, in the case of passwords, payment cards, and billing information, choosing specific credentials or payment card and billing information to store in your Google Account. [Learn More](#).

## How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

**Prerendering.** To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what other people are searching for. [Learn more](#). Predictions can also be based on your browsing history. [Learn more](#).

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more](#).

When you are signed into Chrome with your Google Account, Chrome may offer to save passwords, payment methods and related information to your Google Account. Chrome may also offer you the option of filling passwords and payment methods from your Google Account into web forms. If you have passwords or payment methods saved locally in Chrome, Chrome may prompt you to save them to your Google Account. If you use a payment method from your Google Account or choose to save your payment method in your Google Account for future use, Chrome will collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls](#).

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more](#).

**Usage statistics and crash reports.** By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If

demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on ChromeOS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

## Identifiers in Chrome

to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. ChromeOS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more.](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more.](#)

## Sign-in and Sync Chrome modes

You also have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.



Chrome on Android and iOS, when you sign into any Google web service, Chrome may offer to sign you in with the Google Accounts that are already signed in on the device. You can turn this off in settings. [Learn more](#). If you are signed in to Chrome with your Google Account, Chrome may offer to save your passwords, payment methods and related information to your Google Account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account at [Chrome data from your account](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required for parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable synchronization of most data types. [Learn More](#). The [Privacy Notice for Google Accounts created in Family Link](#) applies to Chrome sync data stored in those accounts.

## How Chrome handles your synced information

Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more](#).

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more](#).

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- **Basic browsing history information** like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

## How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

**Browser configuration changes.** When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this information is saved. These changes are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

---

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system.

[Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for ChromeOS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

---

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about

## How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more](#).

The following Safe Browsing features are specific to Chrome:

- If you have turned on Safe Browsing's Enhanced Protection mode, Chrome provides additional protections, and sends Google additional data, as described in Chrome settings. [Learn more](#). Some of these protections may also be available as standalone features, subject to separate controls, where Standard Protection is enabled.
- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. If you also sync your browsing history without a sync passphrase, these URLs will be temporarily associated with your Google account to provide more personalized protection. This feature is disabled in incognito and guest modes.
- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.

- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).
- On desktop and Android versions of Chrome, you can always choose to [disable the Safe Browsing feature within Chrome settings](#). On iOS versions of Chrome, Apple controls the Safe Browsing technology used by your device and may send data to Safe Browsing providers other than Google.

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

### Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.



sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

123.45.67.89 - 25/Mar/2003 10:15:32 - https://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time they/he visits Google from that particular computer).

## More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.



the [Google Privacy Policy](#). We also comply with certain legal frameworks relating to the transfer of data, including the European frameworks described on our [Data Transfer Frameworks page](#). [Learn more](#).

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

## Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

# **EXHIBIT 134**

**8/11/22  
CHROME  
PRIVACY  
NOTICE**

# Google Chrome Privacy Notice

Last modified: August 11, 2022

View archived versions:

Select date



Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, ChromeOS, and when you enable Safe Browsing in Chrome. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#), as changed from time to time. [Google's retention policy](#) describes how and why Google retains data.

If Google Play apps have been enabled on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the [Google Play Terms of Service](#) and [Google Privacy Policy](#). Details specific to Chrome are provided in this Notice where relevant.

## Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out. We change this Privacy Notice from time to time.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

- [Managing users in Chrome](#)
- [Safe Browsing practices](#)
- [Privacy practices of using apps, extensions, themes, services, and other add-ons](#)
- [More information](#)

## Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

### Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.
- [Cookies](#) or data from websites that you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

- You can [delete your browsing history information](#).
- You can manage or delete stored browsing data from the [Cookies and Site Data dialog](#).
- You can stop Chrome from [accepting cookies](#). [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by turning on sync, or, in the case of passwords, payment cards, and billing information, choosing specific credentials or payment card and billing information to store in your Google Account. [Learn More](#).

## How Chrome handles your information

**Information for website operators.** Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

**Preloading.** You can browse and search faster when Chrome preloads pages that it thinks you might visit. Preloading can be triggered by websites, Android apps, or Chrome itself (e.g., from the omnibox). Preloading can be disabled via Chrome's privacy settings. If preloading is requested, the preloaded site may be allowed to set and read its own cookies just as if you had visited it, even if you don't end up navigating to the preloaded page. In some cases, preloading will be done in a privacy-preserving way, in which case cookies are not sent on requests and they



end-to-end encrypted between Chrome and the preloaded site so that the proxy cannot see the content of the pages. Any information learned by the proxy is used solely to facilitate privacy-preserving preloading and is not linked to other information from your Google account. Privacy-preserving preloading is disabled when in Incognito mode. [Learn more.](#)

**Location.** To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

**Updates.** Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

**Search features.** If you are signed in to a Google site and Google is your default search engine, searches you perform using the omnibox or the search box on the new tab page in Chrome are stored in your Google Account.

**Search prediction service.** To help you find information faster, Chrome uses the prediction service provided by your default search engine to offer likely completions to the text you are typing. When you search using the omnibox or the search box on the new tab page in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. If Google is your default search engine, predictions are based on your own search history, topics related to what you're typing in the omnibox or in the search box on the new tab page, and what

**Navigation assistance.** When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

**Autofill, password management, and payments.** In order to improve Chrome's Autofill and password management services, Chrome sends Google limited, anonymous information about the web forms that you encounter or submit while Autofill or password management is enabled, including a hashed URL of the web page and details of the form's structure. [Learn more.](#)

When you are signed into Chrome with your Google Account, Chrome may offer to save passwords, payment methods and related information to your Google Account. Chrome may also offer you the option of filling passwords and payment methods from your Google Account into web forms. If you have passwords or payment methods saved locally in Chrome, Chrome may prompt you to save them to your Google Account. If you use a payment method from your Google Account or choose to save your payment method in your Google Account for future use, Chrome will collect information about your computer and share it with Google Pay to protect you from fraud and provide the service. If supported by the merchant, Chrome will also allow you to pay using Google Pay.

**Language.** In order to customize your browsing experience based on the languages that you prefer to read, Chrome will keep a count of the most popular languages of the sites you visit. This language preference will be sent to Google to customize your experience in Chrome. If you have turned on Chrome sync, this language profile will be associated with your Google Account and, if you include Chrome history in your Google Web & App Activity, it may be used to personalize your experience in other Google products. [View Activity Controls.](#)

**Web Apps on Android.** On Android devices, if you select "add to homescreen" for a website that has been optimized for [fast, reliable performance on mobile devices](#), then Chrome will use a Google server to create a native Android package for that website on your device. The Android package allows you to interact with the web app as you would with an Android app. For example, the web app will appear in your list of installed apps. [Learn more.](#)

preferences, button clicks, performance statistics, and memory usage. In general, usage statistics do not include web page URLs or personal information, but, if you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google", then Chrome usage statistics include information about the web pages you visit and your usage of them. If you have enabled Chrome sync, Chrome may combine any declared age and gender information from your Google account with our statistics to help us build products better suited for all demographics. For example, we may collect statistics to identify web pages that load slowly. We use this information to improve our products and services, and to give web developers insight into improving their pages. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We may share aggregated, non-personally identifiable information publicly and with partners — like publishers, advertisers or web developers. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

**Media licenses.** Some websites encrypt media to protect against unauthorized access and copying. For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. In the process of allowing access to this media, session identifiers and licenses may be stored locally. These identifiers can be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. For sites that use Adobe Flash Access, Chrome will provide a unique identifier to content partners and websites. The identifier is stored on your system. You can deny this access in the settings under Content Settings, Protected content, and reset the ID using [Clear Browsing Data](#) with "Cookies and other site data" selected. If you access protected content in Chrome on Android, or access higher quality or offline content on ChromeOS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. Your device will share a site specific identifier with the website to certify that its cryptographic keys are protected by Chrome hardware. [Learn more](#).

**Other Google services.** This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter

find more information in the [Chrome Privacy Whitepaper](#).

## Identifiers in Chrome

Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. ChromeOS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more](#).
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more](#).

with or without sync enabled.

**Sign in.** On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. You can turn this off in settings. [Learn more](#). On Chrome on Android and iOS, when you sign into any Google web service, Chrome may offer to sign you in with the Google Accounts that are already signed in on the device. You can turn this off in settings. [Learn more](#). If you are signed in to Chrome with your Google Account, Chrome may offer to save your passwords, payment methods and related information to your Google Account. This personal information will be used and protected in accordance with the [Google Privacy Policy](#).

**Sync.** When you sign in to the Chrome browser or a Chromebook and enable sync with your [Google Account](#), your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

Sync is only enabled if you choose. [Learn More](#). To customize the specific information that you have enabled to sync, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account at [Chrome data from your account](#). On the Dashboard, except for Google Accounts created through Family Link, you can also disable sync and delete all the associated data from Google's servers. [Learn more](#). For Google Accounts created in Family Link, sign-in is required for parent management features, such as website restrictions. However, children with Family Link accounts can still delete their data and disable

## How Chrome handles your synced information

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more.](#)

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt your synced Chrome data with your own sync passphrase. [Learn more.](#)

## Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- [Basic browsing history information](#) like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

## How Chrome handles your incognito or guest information

**Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.



are not affected by incognito or guest mode.

**Permissions.** Permissions you grant in incognito mode are not saved to your existing profile.

**Profile information.** In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

## Managing Users in Chrome

### Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system.

[Learn more.](#)

### Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first starts browsing (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for ChromeOS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

## Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

### How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more](#).

The following Safe Browsing features are specific to Chrome:

- If you have turned on Safe Browsing's Enhanced Protection mode, Chrome provides additional protections, and sends Google additional data, as described in Chrome settings. [Learn more](#). Some of these protections may also be available as standalone features, subject to separate controls, where Standard Protection is enabled.
- If you have turned on "Make searches and browsing better / Sends URLs of pages you visit to Google" and Safe Browsing is enabled, Chrome sends Google the full URL of each site you visit to determine whether that site is safe. If you also sync your browsing history without a sync passphrase, these URLs will be temporarily associated with your Google account to provide more personalized protection. This feature is disabled in incognito and guest modes.

URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware or when Chrome detects unwanted software on your computer. [Learn more](#).
- If you use Chrome's password manager, Safe Browsing checks with Google when you enter any saved password on an uncommon page to protect you from phishing attacks. Chrome does not send your passwords to Google as part of this protection. In addition, Safe Browsing protects your Google Account password. If you enter it on a likely phishing site, Chrome will prompt you to change your Google Account password. If you sync your browsing history, or if you are signed in to your Google Account and choose to notify Google, Chrome will also flag your Google Account as likely phished.
- If you are signed in to your Google Account, Chrome will also warn you when you use a username and password that may have been exposed in a data breach. To check, when you sign in to a site, Chrome sends Google a partial hash of your username and other encrypted information about your password, and Google returns a list of possible matches from known breaches. Chrome uses this list to determine whether your username and password were exposed. Google does not learn your username or password, or whether they were exposed, as part of this process. This feature can be disabled in Chrome settings. [Learn more](#).
- On desktop and Android versions of Chrome, you can always choose to [disable the Safe Browsing feature within Chrome settings](#). On iOS versions of Chrome, Apple controls

## Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

### Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

## Server Log Privacy Information

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry for where the search is for "cars" looks like this, followed by a breakdown of its parts:

123.45.67.89 - 25/Mar/2003 10:15:32 - https://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.;
- 25/Mar/2003 10:15:32 is the date and time of the query.;
- https://www.google.com/search?q=cars is the requested URL, including the search query.;
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.;
- 740674ce2123a969 is the unique cookie ID that was assigned to this particular computer the first time it visited a Google site. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've/s/he visited Google, then it will be the unique cookie ID assigned to their device the user the next time they/s/he visits Google from that particular computer).

---

## More information

including [cookies](#), is subject to the privacy policies of those websites.

Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in the [Google Privacy Policy](#). We also comply with certain legal frameworks relating to the transfer of data, including the European frameworks described on our [Data Transfer Frameworks page](#). [Learn more](#).

---

## Key Terms

### Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

### Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

Follow us





Chrome Family ▼

Enterprise ▼

Education ▼

Dev and Partners ▼

Stay Connected ▼



[Privacy and Terms](#) [About Google](#) [Google Products](#)

[? Help](#) [English - United States](#)

# **EXHIBIT 135**

## **4/14/14 Google Terms of Service**

## GOOGLE TERMS OF SERVICE

Last modified: April 14, 2014 (view archived versions)

# Welcome to Google!

Thanks for using our products and services ("Services"). The Services are provided by Google Inc. ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

By using our Services, you are agreeing to these terms. Please read them carefully.

Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services.

## Using our Services

You must follow any policies made available to you within the Services.

Don't misuse our Services. For example, don't interfere with our Services or try to access them using a method other than the interface and the instructions that we provide. You may use our Services only as permitted by law, including applicable export and re-export control laws and regulations. We may suspend or stop providing our Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct.

Using our Services does not give you ownership of any intellectual property rights in our Services or the content you access. You may not use content from our Services unless you obtain permission from its owner or are otherwise permitted by law. These terms do not grant you the right to use any branding or logos used in our Services. Don't remove, obscure, or alter any legal notices displayed in or along with our Services.

Our Services display some content that is not Google's. This content is the sole responsibility of the entity that makes it available. We may review content to determine whether it is illegal or violates our policies, and

we may remove or refuse to display content that we reasonably believe violates our policies or the law. But that does not necessarily mean that we review content, so please don't assume that we do.

In connection with your use of the Services, we may send you service announcements, administrative messages, and other information. You may opt out of some of those communications.

Some of our Services are available on mobile devices. Do not use such Services in a way that distracts you and prevents you from obeying traffic or safety laws.

## Your Google Account

You may need a Google Account in order to use some of our Services. You may create your own Google Account, or your Google Account may be assigned to you by an administrator, such as your employer or educational institution. If you are using a Google Account assigned to you by an administrator, different or additional terms may apply and your administrator may be able to access or disable your account.

To protect your Google Account, keep your password confidential. You are responsible for the activity that happens on or through your Google Account. Try not to reuse your Google Account password on third-party applications. If you learn of any unauthorized use of your password or Google Account, follow these instructions.

## Privacy and Copyright Protection

Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies.

We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act.

We provide information to help copyright holders manage their intellectual property online. If you think somebody is violating your copyrights and want to notify us, you can find information about submitting notices and Google's policy about responding to notices in our Help Center.

## Your Content in our Services

Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.

If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our Services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account. For example, you can choose your settings so your name and photo do not appear in an ad.

You can find more information about how Google uses and stores content in the privacy policy or additional terms for particular Services. If you submit feedback or suggestions about our Services, we may use your feedback or suggestions without obligation to you.

## About Software in our Services

When a Service requires or includes downloadable software, this software may update automatically on your device once a new version or feature is available. Some Services may let you adjust your automatic update

settings.

Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by these terms. You may not copy, modify, distribute, sell, or lease any part of our Services or included software, nor may you reverse engineer or attempt to extract the source code of that software, unless laws prohibit those restrictions or you have our written permission.

Open source software is important to us. Some software used in our Services may be offered under an open source license that we will make available to you. There may be provisions in the open source license that expressly override some of these terms.

## Modifying and Terminating our Services

We are constantly changing and improving our Services. We may add or remove functionalities or features, and we may suspend or stop a Service altogether.

You can stop using our Services at any time, although we'll be sorry to see you go. Google may also stop providing Services to you, or add or create new limits to our Services at any time.

We believe that you own your data and preserving your access to such data is important. If we discontinue a Service, where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service.

## Our Warranties and Disclaimers

We provide our Services using a commercially reasonable level of skill and care and we hope that you will enjoy using them. But there are certain things that we don't promise about our Services.

OTHER THAN AS EXPRESSLY SET OUT IN THESE TERMS OR ADDITIONAL TERMS, NEITHER GOOGLE NOR ITS SUPPLIERS OR DISTRIBUTORS MAKE ANY SPECIFIC PROMISES ABOUT THE SERVICES. FOR EXAMPLE, WE DON'T MAKE ANY COMMITMENTS ABOUT THE CONTENT WITHIN THE SERVICES, THE SPECIFIC FUNCTIONS OF THE SERVICES, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICES "AS IS".



SOME JURISDICTIONS PROVIDE FOR CERTAIN WARRANTIES, LIKE THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. TO THE EXTENT PERMITTED BY LAW, WE EXCLUDE ALL WARRANTIES.

## Liability for our Services

WHEN PERMITTED BY LAW, GOOGLE, AND GOOGLE'S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA, FINANCIAL LOSSES OR INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES.

TO THE EXTENT PERMITTED BY LAW, THE TOTAL LIABILITY OF GOOGLE, AND ITS SUPPLIERS AND DISTRIBUTORS, FOR ANY CLAIMS UNDER THESE TERMS, INCLUDING FOR ANY IMPLIED WARRANTIES, IS LIMITED TO THE AMOUNT YOU PAID US TO USE THE SERVICES (OR, IF WE CHOOSE, TO SUPPLYING YOU THE SERVICES AGAIN).

IN ALL CASES, GOOGLE, AND ITS SUPPLIERS AND DISTRIBUTORS, WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE THAT IS NOT REASONABLY FORESEEABLE.

## Business uses of our Services

If you are using our Services on behalf of a business, that business accepts these terms. It will hold harmless and indemnify Google and its affiliates, officers, agents, and employees from any claim, suit or action arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, suits, judgments, litigation costs and attorneys' fees.

## About these Terms

We may modify these terms or any additional terms that apply to a Service to, for example, reflect changes to the law or changes to our Services. You should look at the terms regularly. We'll post notice of modifications to these terms on this page. We'll post notice of modified additional terms in the applicable Service. Changes will not apply retroactively and will become effective no sooner than fourteen days after they are posted. However, changes addressing new functions for a Service or changes made for legal

reasons will be effective immediately. If you do not agree to the modified terms for a Service, you should discontinue your use of that Service.

If there is a conflict between these terms and the additional terms, the additional terms will control for that conflict.

These terms control the relationship between Google and you. They do not create any third party beneficiary rights.

If you do not comply with these terms, and we don't take action right away, this doesn't mean that we are giving up any rights that we may have (such as taking action in the future).

If it turns out that a particular term is not enforceable, this will not affect any other terms.

The laws of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services. All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

For information about how to contact Google, please visit our [contact page](#).